# Impact on NATO of Cyberspace as a Domain of Operations

## A SWOT Analysis

Alžběta Bajerová

## Table of Contents

## 1. Introduction

In July 2016 at the Warsaw summit, NATO recognised a new domain of operations: cyberspace. In doing so, NATO sought to 'improve its ability to protect and conduct operations across all the domains and maintain its freedom of action and decision', as stated in the Warsaw Summit Communiqué (2016). However, such a strategically significant step may bring with it a variety of unanticipated outcomes.

The development of cyberspace, with its threats and opportunities, has been extremely fast. The policy sector has been desperately trying to keep up while an entirely new domain was swiftly establishing itself without any major non-technological academic debate whirling in its background. As a result, from the strategic perspective we can see many uncharted and unconsidered areas in the cyber domain that may result in unwelcome outcomes as NATO moves further forward in defence development.

The main goal of this paper is to map the non-technological challenges that stem from recognising cyberspace as a domain of operations, to shed a light on the uncertainties that surround its recent development, and to make a few recommendations based on the arguments that will be made along the way.

To do so in a simple and explorative manner that will give us space for broader debate, the paper will follow the framework of a SWOT analysis, while omitting the final SWOT matrix and exchanging it for a summarising conclusion and set of recommendations based on previous analysis. SWOT is a method based on analysing multiple internal and external factors, establishing the main *strengths, weaknesses, opportunities* and *threats* in the strategic process. A selected approach is used for evaluation, and for the foundation and design of strategies and policies. (Verboncu and Condurache 2016).

This paper will apply the SWOT framework to the possible effects of cyberspace becoming a domain of operations. Through the subsequent analysis, we will be approaching the answer to a complex question: *What is the possible future effect on NATO of recognising cyberspace as a domain of operations?* However, since it is not possible to answer such a question succinctly and with certainty, the main product of this paper will thus not be a simple one-line answer, but a set of arguments made along the way while considering the question. The role of the arguments will be not only to unveil possible directions for NATO in the cyber domain, but also to challenge current paradigmatic views on cyberspace and prompt a debate on the non-technological aspects of the new domain.

## 2. SWOT – Strengths

### 2.1. Enhanced cooperation

Giving cyberspace the status of a domain encompasses a strong integrative element, on several levels. First, it embeds cyberspace deeply into the military ethos. Amplifying the interconnection between military and "cyber", while giving cyberspace more approachable façade of a "domain of operations", might positively effect governments perception of the area. Although strengthening the Alliance is desirable in all domains, calls for stronger defence measures in cyberspace are even louder due to presence of states which so far have not successfully developed adequate cyber security measures. Change in the perception of

cyberspace resulting from its new label of a domain of operations might thus prompt a change in governments' behaviour regarding spending on cyber security and cyber defence, particularly in member states that so far have been reluctant to take any defensive measures in cyberspace. Therefore, we might witness increased development of cyber capabilities within the Alliance and allocation of larger financial and personnel resources to this area.

Second, the pathway towards the desired development of a secure cyberspace is greatly helped by the strong discourse of cooperation that NATO has adopted alongside of establishing the new domain. When the more developed allies help other states to increase their defensive ability, it is possible to move more quickly towards achieving the NATO goal of ensuring the ability to protect and conduct operations in cyberspace (and in air, space, land and maritime where a cyber element plays an important role) to maintain our freedom of action and decision.

The commitment to mutual help in the cyber domain, not only for NATO members but also partners, is not an empty promise. Ukraine has received special cyber equipment from NATO to counter the cyber attacks that the state is currently facing. (Oliphant, 2017) The Asia Pacific Computer Emergency Response Team and the NATO Rapid Reaction Team (RRT) are another example of existing multilateral arrangements to provide support to states that are coping with hostile cyber operations.

Third, the new greater emphasis on development and interaction that accompanies the establishment of the fifth domain in turn adds to strengthening mutual trust amongst NATO members and partners, creating a fruitful environment for bolstering cooperation in cyberspace.

### 2.2. Stronger emphasis on the cyber element

Article 2 of the Cyber Defence Pledge, a document signed by the Allies at Warsaw Summit 2016, openly addresses the interconnectedness that calls for cooperation in the protection of NATO's networks, and assurance of its operations. The latter is especially important. Cyberspace is not just a realm on its own, it is also an element partially present in all the physical domains of operations. It underlies nearly all the physical means of warfare, and its presence within is increasing. Therefore, although we might worry about a 'cyber war', what is really coming is the age of 'cybered warfare',[1] that is, warfare in all domains underpinned by extensive operations of cyber nature (Dombrowski and Demchak, 2014).

Cyber capabilities provide a great potential when it comes to operations. They represent a more moderate alternative to physical measures such as the use of ballistic missiles or drone strikes. Their generally less destructive nature makes cyber capabilities a healthy choice for an Alliance like NATO that abides by international law.

Establishing cyberspace as a domain means acknowledging the importance of securing the cyber element that is present in warfare today, and it also gives the Alliance the chance to

[1] A term developed by Dombrowski and Demchak (2014). In their paper *Cyber War, Cybered Conflic, and the Maritime Domain*, the authors oppose the term 'cyber warfare' and insist that no such thing as conflict limited to cyberspace will occur, and the whole concept only distorts our perception of cyberspace. They call for an embrace of the true domain-underlying nature of cyberspace and to reflect this nature through using correct terminology. Thus, they propose to replace the limiting term 'cyber warfare' with a broader, domain-cutting term 'cybered warfare'.

embrace the full potential of the cyber domain, for example through development of new cyber capabilities. By formally approaching cyberspace as a domain, the Alliance will be better able to coordinate development in peacetime and to prepare and cooperate during operations.

Making cyberspace a domain is also an important signal for particular members of the Alliance. That is not to underestimate the role that the cyber element plays in national security and during operations, as there are still voices that diminish cyberspace's validity in both state security and mission assurance, or emptily acknowledge its importance without taking any actual steps towards its protection.

### 2.3. Stronger deterrence

Making cyberspace a domain is not just a message for NATO's members and partners, it is also a signal to NATO's possible adversaries. It implies that, if necessary, the Alliance is willing and prepared to defend itself on all fronts, cyberspace included. This message therefore carries a significant deterrent potential. NATO's open commitment to invoke Article 5 in response to a severe cyber-attack, and commitment to continuous improvement of the Alliance's defence ability, further strengthen the deterrent message. (Wales Summit Declaration 2014, Article 72)

During my research, I have quite often came across a shared apprehension: *Will the Alliance's effort to strengthen its capabilities in cyberspace create tension or even security dilemma?* In my opinion, such scenario is unlikely. Developing cyber capabilities does not change the defensive mandate of NATO in any way. Such efforts are no different from development of any other type of military capabilities. The Alliance, as well as other states, creates a new range of capabilities in a newly developed domain, in order to continue fulfilling its goal to protect its members.

If the Alliance ignored the increasing importance of the cyber element in warfare and thus left cyberspace unprotected, the Alliance's defensive potential would not stay the same – it would diminish significantly over time. A weakening of the Alliance would subsequently cause a range of unpleasant political consequences, including a lower deterrent potential of NATO as a whole. To maintain the status quo, NATO must act on the need for development of capabilities in cyberspace.

Simply put, NATO needs to close the cyberspace fissure that was opening up in its defensive bulwark. The decision to establish cyberspace as a new domain of operations was in line with this need, although it cannot stop there.

## 3. SWOT – Weaknesses

Although elevating cyberspace to a domain of operations has its positives, their influence is being diminished by weaknesses in NATO's current approach to the domain. This paper has identified four such weaknesses.

### 3.1. Lack of trust and unity

One of the major problems NATO is facing today is a sense of distrust amongst its members that results in disunity of the Alliance. Such disunity in turn creates further distrust. This vicious circle has several negative effects that are presented below.

### 3.1.1. Collective defence

One of the mistrust-related problems is the question of Article 5, which is inherent to all the physical domains and was inherited by cyberspace. It is the broad question of trust in the willingness of NATO members and partners to stand up for one another's defence. Article 72 of the Wales Summit Declaration, a document in which NATO first defined its cyber policy in 2014, concludes that a cyber attack might lead to the invocation of Article 5, but any decision shall be made on case-by-case basis. This statement was further confirmed by NATO officials at the 2017 International Conference on Cyber Conflict (CyCon) in Estonia (*Defense News*, 2017). The *Tallinn Manual 2.0* also works with the possibility of collective defence triggered by cyber attack; Rules 74 and 75 govern the process and set its limits within international law. However, one question still remains unanswered: what attributes must a cyber attack have in order to trigger collective defence?

For now, the threshold for collective defence is defined by each NATO member separately. That means there are 29 different red lines, which is another example of disunity within the Alliance that might result in complications as soon as one or more members are hit by a major cyber attack. In that moment, the targeted country or countries would face the challenge of persuading allies that the scale and effects of a cyber attack were grave enough to trigger Article 5. Not only would collective defence have to be discussed; there would need to be discussion about the very right of self-defence against the presumed attacker under the UN Charter.

Some authors propose to solve this problem by unifying the threshold. For example, Cathrine Lotrionte of Georgetown University argues: 'Most attacks in cyberspace use no force. We would need to have a legal threshold for such threat situations,' (*Defense News*, 2017). Yet, acting on such a proposal for a collective definition of 'the red line', if only amongst NATO members, would be complicated.

As Clare Lain from NATO CCD COE argues, defining one common threshold for all the 29 states could be a strategic mistake. It would strip the member governments of the right to define their own threshold of unacceptable behaviour. Although a possible consensus could be discussed at a NATO level, it is highly unlikely that it would be reached unanimously. Second, reaching such a consensus could have negative political consequences. Defining an official threshold might result in legitimisation of all other attacks which do not cross that threshold, and even unwittingly prompt such behaviour. Therefore, in the case of Article 5, the disunity seems inherent and unresolvable.

The question of willingness to respond collectively to an attack on a member state is core for all the physical domains. However, in cyberspace it seems particularly problematic because of the nature of cyber attacks, as they usually do not cause any harm in the physical world. Therefore, although they might have serious consequences of a cyber nature, their severity might not be apparent. As Michael Turner (2013) from the University of Cambridge puts it:

> 'The difference is that the direct effects of the attacks don't result in explosions and loud noises, instead they subtly affect devices connected to cyberspace, and so it's easy to be fooled into thinking that cyber attacks are not violent.'

This characteristic of cyber attacks makes them less approachable for decision-makers and political actors in general, causing NATO members to be less willing to respond collectively,

if at all, to a cyber attack. This uncertainty and insufficient comprehension in turn creates doubts about other allies' willingness to invoke collective defence following a cyber attack, which further strengthens the trust gap between members in the fifth domain and contributes to further division of the Alliance.

#### 3.1.2. Secretive environment

Another problem stemming from the lack of trust and unity is the level of overall secrecy amongst NATO members regarding various aspects of cyber operations. Although NATO has declared a whole new domain of operations, there is a little willingness to clarify how the actual operations will be carried out. Retired US General Michael Hayden addressed the issue of 'over-classification' in the US Army as follows:

> 'American industry hides the ball from one another and from the public for fiduciary reasons, and the American government hides the same ball because of the hideous over-classification of cyber-related information' (Takala, 2015).

Such secrecy of individual allies subsequently spreads up to transnational level and into NATO.

Due to unwillingness to share cyber-related knowledge in general, and particularly about the development and use of various cyber capabilities during operations, the defensive and operational potential of NATO is being diminished. This problem is further amplified by the fact that the cyber domain underlies all the physical domains and the presence of the cyber element in physical warfare will only increase over time. The excessive secrecy thus threatens to negatively influence the military operations in all other four domains as well.

The impact of the mutual distrust on the creation of the secrecy issue is substantial. Sharing one's knowledge about certain elements of cyber defence typically means sharing information on one's own vulnerabilities. States may be worried that any information shared might be exploited by other nations for espionage or other malign purposes. Besides, there is a possibility that information shared within NATO might be seized by a third party, as not all NATO members possess the cyber equipment necessary for protecting sensitive information.

### 3.2. The attribution problem

Reactive possibilities in the new domain are further hindered by the 'attribution problem' – the complicated and uncertain attribution of attacks to the respective attackers in cyberspace. Most high-level attackers are more than capable of hiding their origins, and even with advanced forensic techniques it is often impossible to identify the attacker with certainty. Even when tracking the attack to the country of its origin, it can be impossible to prove conclusively whether a certain group of hackers was acting under the government's command or on their own account. (Farrell, 2014)

The problematic practice of attack attribution speaks for itself. It took less than 24 hours for a prominent cybersecurity expert to cast a doubt on claims by unnamed US officials that China was behind the breach of OPM's networks in 2015. (Segal, 2015; Knake, 2015; Davis, 2015) Official accounts of Pyongyang's role in the Sony attack played out similarly, with news outlets featuring competing expert accounts of responsibility and a line-up of suspects that included North Koreans, Russians, hacktivists, cyber criminals, and disgruntled employees. (Segal, 2015; PBS, 2014)

Even when identifying the attackers, a legal dimension of attribution enters the frame. Can the actions of a hacker be attributed to a nation-state as a matter of law? Answering this question presents a major legal hurdle if the attack is launched by an ostensibly non-state hacker with murky ties to an adversary government (Segal, 2015). The burden of attributing the actions of non-state hackers to a state would be substantial.

Unfortunately, the attribution problem has serious consequences for the allies' ability to respond to an attack. Even if there is a solid amount of evidence to identify the attacker, since the proof is inherently fallible, the legitimacy of any potential response in insufficient. As the suspected attacking country will most likely deny carrying out the attack, the question of responsibility for such action will shift from forensic analysis to a political game. Under such pressure and with limited legitimacy of the accusation, the affected state (or the Alliance) will be much less likely to respond. Thus, the attribution problem reduces the likelihood of a response, what makes the cyber domain a soft spot in the Alliance's defence.

### 3.3. Capability gap

*'Our interconnectedness means that we are only as strong as our weakest link.'* – NATO Cyber Defence Pledge 2016, Article 2

There are differences in the abilities of NATO members to defend themselves in cyberspace and to provide cyber mission assurance for the Alliance. Although there are, and always will be, differences in general military competence caused by varied economic strength or political will, the current low level of cyber literacy and lack of ambition to raise it is a common phenomenon for a number of NATO members. Due to the interconnectedness of the Alliance, the capability gap represents not just a threat to allies, but a threat to the cyber defence of NATO as a whole. This setup leaves NATO's new domain protractedly semi-protected, while it is simultaneously facing the fast-paced development of cyber threats. The inability of certain allies to secure their cyberspace might thus draw in potential adversaries.

Moreover, the capability gap strengthens the above-mentioned environment of secrecy. A state that cannot be trusted to protect information is much less likely to receive such information. In a broader sense, it means that the capability gap reinforces the dysfunctional environment of distrust and discord.

### 3.4. Insufficient non-technological comprehension of cyberspace

There is a fourth weakness to the cyber domain that so far has remained largely unaddressed by the strategic community. It is the relative gap in non-technological knowledge of the new domain. The lack of theory and non-tech concepts results in harmful ambiguity in the political cyber security debate within NATO.

The technological development of cyberspace is extremely fast-paced. NATO members and their governments are trying to keep up with the ever-evolving threats posed by a great variety of actors. The political sphere finds itself under great pressure to respond as quickly as possible, and we have witnessed a speedy process of 'securitisation', i.e. the process of extreme politicisation where the issue is presented as a threat that requires security measures being taken outside the normal political procedure (Buzan et al., 1998). However, in the rush to catch up with technological developments, the political sphere has outrun the non-technological knowledge in the field. It might be partially because the need for securitisation

of cyberspace is a rather uncontroversial topic, thus it has not provoked any great non-technological debate that would have produced a deeper understanding of the area. Nevertheless, we are now left with a new and very specific domain of operations that we are not quite able to intellectually grasp at the non-technological level.

Current vagueness, ambiguity or even inaccuracy in strategic debate about cyberspace produces an environment of uncertainty in NATO's political sphere, which increases the distrust amongst allies and reduces the probability that decision-makers will opt for cyber solutions during operations.

## 4. SWOT – Opportunities

### 4.1. Accelerated development and use

Recognising cyberspace as a domain means a greater possibility to accelerate development in this area. The creation of a new domain has generated momentum in the political sphere, which NATO members can use to push for greater financial and human resources for the area. Through subsequent accelerated development in cyberspace, NATO's defence will become stronger, as the cyber domain underlies the physical ones.

Acknowledging cyberspace as a vital part of the military ethos is a great opportunity for NATO to expand its arsenal of capabilities when it comes to mission assurance. Cyber capabilities are in general less destructive than kinetic ones, thus carrying less political and financial cost. That makes them an ideal instrument for the mission assurance purposes of NATO, an organisation with a defensive mandate, abiding by the norms of international law.

The full potential of cyber capabilities during operations has not yet been fulfilled, as there is a natural drift towards the well-known kinetic options. Granting cyberspace the status of a domain may result in an emphasis on the use of its capabilities, further exploration of their potential for mission assurance, and subsequently a greater willingness to opt for them during operations.

### 4.2. Reduction of the capability gap

If this opportunity is taken, it might also contribute to reducing the capability gap between member states. As described in Section 2, recognising cyberspace as a domain elevates the importance of cyberspace, outlining its relevance for the Alliance's overall security. This might create additional pressure on national representatives to stop taking cyber defence lightly and start committing resources to its development. It might represent a further pressure on states that have not put enough resources into developments in cyberspace to adopt a more pro-active approach, and signal to the governments of the weak-link states that ignoring developments in cyberspace is no longer an option.

Such increased emphasis should ideally meet the current cooperative discourse of the Alliance and its willingness to help the 'cyber under-developed' states. If the weak-link states take up this opportunity to improve, NATO could form a strong cyber alliance of 29 cyber-capable states, which will able to resist and effectively deal with any future threats.

### 4.3. Reduction of secrecy

Many scholars called for an open discussion about various elements of cyberspace long before it became a domain of operations; such voices are now becoming stronger and more numerous. Our new ability to compare cyberspace with other domains has shed a light onto its overly secretive environment or 'over-classification'. In cyberspace, many issues are still taboo, and vast portions of information are still being withheld, although their equivalents in the physical world are discussed commonly between allies. A consistent push towards greater openness and information-sharing will hopefully reduce the level of secrecy that currently hinders both development in the new domain and trust amongst allies.

A reduction of secrecy might also be achieved by levelling the capabilities of member states. An increase in the abilities of member states to protect sensitive information from alien parties might lead to at least slight progress in openness within the Alliance. From a broader perspective, unifying the abilities of member states might result in increased trust within the Alliance.

A reduction in the level of secrecy will also further contribute to overall increased development in the domain. Through open conversations, development of cyber capabilities, and their use, allies will have a chance to increase their defensive potential in cyberspace.

### 4.4. Enhancement of non-technological knowledge of cyberspace

Success in all the aforementioned opportunities lies in the ability to correctly grasp the topics on the political level, as future decisions regarding the new domain will be political. Thus, to fully seize the opportunities, it is necessary to enhance the comprehension of cyberspace and its various concepts and clear up the confusion that now limits the non-technological strategic and political grasp of the new domain.

By using the new-found political interest in the topic that was created by recognising cyberspace as a domain, NATO has an excellent opportunity to prompt a new wave of non-technological academic debate on cyberspace and its underlying concepts. Through enhancing non-tech knowledge of cyberspace, decision-makers and the political sphere in general will possess a better comprehension of cyberspace that will allow them to make more informed decisions.

Facilitated translation of technological means to political narratives could also lead towards greater willingness of allies to opt for cyber capabilities during operations. Moreover, if NATO manages to increase non-technological comprehension of cyberspace, the current harmful environment of uncertainty and ambiguity will be significantly reduced.

## 5. SWOT – Threats

### 5.1. Loss of unity

As a first weakness, the paper has identified the lack of trust and unity within the Alliance. Uncertainty regarding whether the allies will be willing to defend one another is common to all the physical domains; its effect in cyberspace, however, seems to be magnified by the current state of affairs. Although allies have declared their willingness to stand in defence of one another even in case of cyber attack, current strategic ambiguity causes a notable absence of viable strategy for such a case.

While responding to a cyber attack with kinetic means might be considered too escalatory for the majority of cases, response by cyber means cannot be considered either, as none of the states are currently willing to talk openly about deployment of such countermeasures. Unfortunately, none of the less intense responsive options, such as political and economic sanctions, have been openly discussed either up to this point. That means that there are currently no consequences for a cyber attack on a NATO member or partner.

Rising doubts might be further strengthened by the omnipresent lack of trust amongst members when it comes to developments in cyberspace, manifested by withholding information, particularly regarding cyber capabilities. Lewis (2015) views NATO members' secrecy about their capabilities as a threat, as it increases the 'likelihood of opponents miscalculating as they consider the risk of using force or coercion against NATO members or interests.' Lewis argues that potential adversaries might be more likely to attack in cyberspace, as the nature of NATO's response to the attack in this domain (and its willingness to do so) is still a little blurry in comparison to other domains. Of course, one might argue that, following the policy of strategic ambiguity, the same level of ambiguity might also result in adversaries miscalculating 'the other way', therefore being actually less likely to carry out a cyber attack on NATO. However, this policy is risky and stability-undermining in general, while the current lack of NATO's reaction to any attacks in cyberspace is bending the odds towards making the secrecy more a threat than an advantage.

Regarding relations within the Alliance, the effect of secrecy is damaging. It undermines trust between allies, hinders their ability to cooperate effectively, and distorts the unity of NATO as a whole. Unfortunately, the existence of this harmful secrecy cannot easily be dismissed, as it has a strong reasoning behind it. Sharing information regarding various elements of cyberspace is potentially hazardous as it might be used for malign purposes. In the past we have witnessed many cyber espionage scandals,[2] therefore states' endeavour to conceal vulnerabilities and capabilities is perceivable as rational. This reveals another level of mistrust amongst allies; cyberspace makes it cheaper and easier for states to exploit or eavesdrop on one another, and therefore contributes to mistrust within the Alliance.

Unless the mistrust within the Alliance is overcome by stronger pressure for cooperation in cyberspace, it might result in a gradual weakening of NATO's defensive ability in this domain. Even if such a scenario was limited only to cyberspace, weakness in this domain would inevitably result in hindered mission assurance in general and weakened security of the allies during peacetime, as cyberspace intersects all the physical domains. It is also possible that increased mistrust when it comes to cyberspace would spill over to the political level and hinder cooperation within NATO in general. Such a half-dissolved Alliance would then not be fully able to deter attacks and defend itself.

### 5.2. Lack of response to cyber attacks

The current unwillingness to respond to cyber attacks by any means – not just by kinetic or cyber, but also political or economic – encourages the already present doubt amongst members and partners that allies will not stand up for them in case of an attack, especially if the attack is carried out in cyberspace. This is compounded by the attribution problem. It is therefore possible that in future the attribution argument will stand in the way of activation

[2] Such as the revelation of the US spying on Germany (2015) or Germany spying on the US (2017)

of collective defence, or even the right to self-defence against a cyber attack under the UN Charter. For that reason, the attribution problem has the potential to become one of the most destabilising elements in the cyber domain.

The attribution problem prevents states from effectively responding to an attack, and the weak spot that cyberspace it represents may attract possible adversaries. If the attribution problem will make any response to a cyber attack impossible, cyberspace would quickly become a domain-of-choice for adversaries to conduct offensive operations, as they will not have to fear consequences of any kind from NATO. The attribution problem could thus both contribute to the paralysis of NATO members' ability to respond to cyber attacks and simultaneously increase their frequency.

### 5.3. Widening of the capability gap

Due to the interconnectedness of cyberspace amongst NATO allies in particular, the cyber capability gap represents a significant threat, not just to the weaker states, but to the Alliance as a whole. The weak-link states might suffer from sensitive data theft by foreign adversary, or create an entry point for malware during peacetime or operations. Such states might reasonably be perceived as an easy target by potential adversaries, thus their weakness in cyber domain also heightens the risk of suffering from cyber attack.

NATO can close the capability gap in cyberspace. In many strategic documents, including the Cyber Defence Pledge (2016), allies have stated their willingness to meet the obligations of mutual support, while they cherish a discourse of cooperation. The less-capable allies have also had the opportunity to see the authenticity of such a promise, when more-capable NATO members provided Ukraine with some vital equipment after the cyber attack in 2017. However, in the end it is the weak-link states themselves which have to assume responsibility and start developing cyber measures for their (and the Alliance's) protection. If their governments will not acknowledge the problem and refuse to allocate resources to the development of cyber security and defence, any form of help will prove futile.

NATO can only suggest, but not command. So far, the organisation struggles to get Allies to comply with the agreed 2% budget military spending. If NATO fails to convince its members about the importance of development in cyberspace and the need to allocate both financial and human resources accordingly, the capability gap will deepen even further. In that case, NATO's ability to defend and deter will gradually weaken, as the new domain will become increasingly unguarded and exposed to new threats.

### 5.4. Continuing non-technological incomprehension and lack of concepts

A very specific and somewhat unrecognised threat is formed by the widespread lack of comprehension of the non-technological aspects of the cyber domain. Although the absence of a functional non-technological theory in a technology-dominated domain might seem a second-tier problem, in fact the inability to accurately understand various aspects of cyberspace (such as the concepts of cyber attack, cyber warfare, deterrence or cyber weapons) affects the language of NATO's most important strategic documents. Those materials subsequently guide the development of new measures, allocation of financial resources and the general direction of further development.

By using unclear or misplaced concepts to draft these strategies, NATO itself hampers its full potential to defend and deter, or even diminishes its operational ability (for example, through a distorted view of the concept of cyber capabilities). The same concepts and documents are used to draft policies, and therefore might inflict damage on the international position of NATO (for example through a distorted view of the concept of deterrence). The overall environment of uncertainty and ambiguity may make it less likely for decision-makers to deploy cyber capabilities during operations, as they will prefer to opt for 'familiar' kinetic measures instead, although the cyber option might in certain situations deliver fewer casualties and lower political and financial costs.

With cyberspace becoming a domain of operations, the existing conceptual gap has been pasted over with the label of a 'domain'. Subsequently, a spill-over of concepts from the physical domains occurred as a result of an endeavour to fill in the non-technological intelligence gap in the cyber defence area. These adopted concepts, however, have mostly not contributed to a clarification of the domain's workings and functions. The cyber domain has an enormous number of specifics that simply cannot be adequately reflected by concepts derived from the physical world. Widely used parallels, such as the comparison of cyber and nuclear weapons, usually distort the reality of cyberspace, suppressing its specifics rather than acknowledging them, in order to fit into the boundaries of the desired concept.

In the following section, the paper will discuss the dangers of using such ambiguous or misplaced concepts in strategic processes by offering two practical examples – concepts of cyber deterrence and cyber capabilities. With these cases, the paper hopes to prove the validity of the argument that calls for enhancement of non-technological knowledge in cyber domain area.

### 5.4.1. The concept of cyber deterrence

Deterrence is the ability to create a perception in the mind of adversaries that one has the capacity to impose significant harm on them or to limit their possible gains, should they undertake offensive action. It is an inherently coercive component of strategy that involves 'the potential or actual application of force to influence the action of a voluntary agent' (Freedman, 2004).

Deterrence seeks to dissuade the actor from pursuing violent behaviour in the first place. It does so by altering the actor's cost-benefit assessments of the various strategic choices available. If an actor perceives that the expected utility of a given action is outweighed by the likely costs, they will be deterred from behaving in that fashion, thereby preserving the status quo. (Muller and Stevens, 2017)

There are two general approaches towards deterrence: deterrence by denial and deterrence by punishment. Deterrence by denial relies on the defender's ability to protect itself so perfectly that it makes it impossible for the adversary to carry out a successful attack. It denies the adversary's desired ends, thus makes the very act of attacking useless. (Snyder, 1961) Deterrence by denial might seem the right choice for cyberspace, when considering NATO's defensive purpose. However, no network or system can be *absolutely* secure against cyber attacks or incidents. Achieving such a high level of protection that it would deny the very possibility to attack is thought to be impossible by many authors (Pernik, 2016; Tor, 2015; Denning, 2015; Lewis, 2015)

Deterrence by punishment is based on a threat of massive retaliation that would be launched against any hypothetical adversary, should it attack. Its success is based on a credible threat stemming from the ability to carry out such retaliation (Snyder, 1961). In cyberspace, deterrence by punishment would be relying on NATO's response using cyber capabilities, kinetic means, or political, economic or financial sanctions. The use of kinetic means to respond to a cyber attack is usually viewed as an excessive escalation that NATO would hesitate to use, thus it fails as a credible deterrent. Political, economic or financial sanctions as a response to a cyber attack have not yet been officially articulated, and it is arguable whether their potential impact might serve as a 'massive' retaliation in case of a strong cyber attack. Literature about cyber deterrence therefore usually gravitates towards the necessity of developing cyber capabilities that would serve as a response in case of cyber attack on NATO members, thus deterring the adversary's motivation to carry out such an attack in the first place.

However, there is a fundamental problem underlying both approaches, which stems from our comprehension of the concept of deterrence as a whole. The US's (and subsequently NATO's) approach to deterrence was developed in the nuclear context of the Cold War and is *absolute* in nature – that is, aiming for zero acts of nuclear violence (Tor, 2015) With deterrence by punishment, where the retaliatory act is part of the equation, the initial attack entails the collapse of the deterrence as such, marking a shift towards coercion and the start of a conflict. Due to this *absolute* nature of our current approach to the concept of deterrence, the application of this concept in the cyber domain is inaccurate. Cyber attacks are already omnipresent.

The problematic application of the concept leads us to similarly incompatible parallel between nuclear weapons and cyber capabilities. Many officials of various nations (such as former US Secretary of State John Kerry, Russian Deputy Prime Minister Dmitry Rogozin, Chief of General Staff of the People's Liberation Army of China, General Fang Fenghui, US National Security Advisor Brent Snowcroft, Admiral Michael Rogers of the US Cyber Command or Director of the US National Intelligence James Clapper; for references see Cirenza 2016) have all presented the threat posed by cyber weapons as comparable to, or in some cases greater than, that of nuclear weapons. Same narrative is also upheld by some authors (i.e. Shackelford 2009), other ones use the analogy between cyber and nuclear warfare to derive conclusions for strategic concepts such as deterrence (i.e. Kramer 2016)

However, cyber capabilities do not have the characteristics that made nuclear weapons a strategic deterrent. First, the ability of destruction does not reach the same level. Although it is possible to theorize over a scenario when cyber weapons are used to hijack nuclear missiles and carry out an attack, any major physical damage caused directly by cyber weapons has not yet taken place. Therefore, nuclear-level destruction inflicted by cyber capabilities fails as a credible deterrent. Second, unlike nuclear attacks, cyber attacks are omnipresent; hundreds of attacks are being carried out on a daily basis by attackers of various backgrounds, using cyber capabilities of various strength. It is therefore impossible to view cyber capabilities in general as being able to deter cyber attacks in an absolute manner, either by punishment or by denial. The ubiquity of cyber attacks of various ranges and strengths makes it impossible to fit them into one *absolute* concept built on an enormous destructive power such as that of nuclear weapons.

If NATO allies continue to approach cyber deterrence in the same way as nuclear deterrence and decide to develop cyber capabilities with overwhelming retaliatory capacity in to deter attacks by punishment, it would be unclear what kind of attacks those capabilities would be responding to. NATO members are facing many attacks of different magnitude every day. Endeavor to deter a constantly occurring phenomenon by the use of massive force is simply not credible enough for successful deterrence by punishment.

Therefore, if NATO wishes to develop credible deterrence for cyberspace, it needs to approach the entire concept with an acknowledgement of the specifics of the new domain. That is, amongst others, accepting the low level of damage that cyber attacks typically inflict, as well as the fact that cyber attacks and incidents are occurring frequently, with great variety of strengths, caused by a great variety of actors. Therefore, this paper argues, it is necessary to give up the absolute, nuclear-related parallel.

Uri Tor from the Interdisciplinary Centre in Herzliya, Israel, proposes an alternative approach to cyber deterrence. Author's titled *Cumulative Deterrence as a New Paradigm for Cyber Deterrence* (2015) offers an Israeli perception of deterrence, where the occasional mutual use of force of a flexible magnitude is accepted and even viewed as necessary to maintain an effective deterrence posture, rather than as a failure of deterrence. By occasionally clashing, states are mutually assuring themselves of their willingness and ability to defend.

This approach is not proposed as the right answer for the NATO's question of deterrence in the cyber domain, perhaps due to a possible clash with the defensive mandate of the Alliance. Tor's alternative, however, can at least serve as an example that it is possible to find other, perhaps more fitting ways of approaching the conceptual challenges of cyberspace by looking outside the current physical domain's paradigms.

### 5.4.2. The concept of 'offensive' cyber capabilities

NATO's Strategic Concept of 2010 promises that the Alliance 'will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations'. Some scholars claim that, although NATO's mandate is defensive, without the development of so-called offensive cyber capabilities – capabilities able to disable, distort or destroy adversaries' systems – the Alliance would be left in a reactive mode, thus not being fully able to ensure both abilities listed in the strategic concept. The development of such capabilities in cyberspace, however, represents a sensitive political issue. Although the US is starting to open the conversation about offensive cyber operations, particularly towards terrorists (Ackerman, 2016), questions about the use and development of 'offensive' cyber capabilities still represent a taboo for many states.

NATO members and partners have been overly secretive about the development or use of any cyber capabilities that might not serve only as a passive shield. This results in uncertainty surrounding the topic, which has had multiple negative effects, such as an increased likelihood of opponents miscalculating their risk of using force against NATO, undercutting the legitimacy of NATO operations by failing to build public understanding, and seeing NATO left open to charges of sinister plots (Lewis, 2015). A question that outside experts have posed for a decade is: if we could have a robust discussion of nuclear strategy and capabilities, why can't we have the same discussion about cyber capabilities? (Lewis, 2016)

This paper argues that this secrecy might be caused, amongst other reasons, by incomprehension of the very concept of 'offensive cyber capabilities', or 'cyber capabilities' in general.

Possessing capabilities with offensive potential that are intended for neutral or defensive purposes is standard for NATO in all physical domains. Military capabilities owned by allies, such as warships, aircrafts and ballistic missiles, are crucial for assuring NATO's ability to defend and deter, and for mission assurance in general. The use of such capabilities in conflict would technologically be 'offensive' (destroying, distorting, or disrupting tactical and strategic targets on the opponent's side), yet they are not primarily labelled as such. When it comes to physical capabilities, NATO emphasises its strictly defensive mandate, which prohibits the use of such capabilities for other than defensive purposes, peace-keeping operations, or other activities of a peaceful nature such as transportation. The same mandate applies to the cyber domain and its respective capabilities. It is therefore unnecessarily harmful to label cyber capabilities in general as 'offensive.' Words do have power and international diplomacy is highly sensitive to them. Therefore, putting an outwardly aggressive label on a group of capabilities might be enough to prevent NATO, a strictly defence-oriented and highly political organisation, from discussing their existence or development.

The label 'offensive' is not only unnecessary, many times it is also incorrect. Just as in the physical world various capabilities can be used to 'do both good and evil' according to the user's intent, the same principle applies to cyberspace. Cyber capabilities are tools, whose nature is mostly neutral. Whether they help or harm, attack or defend, depends solely on their use.

One example of such cyber capability is Nmap (Network Mapper), a free and open source utility for network discovery and security auditing. However, the same piece of code is commonly used for discovering and exploiting vulnerabilities or launching DoS attacks. (Occupy4elles, 2016) Another example is Scapy, an interactive packet manipulation program that can be very useful for unit tests, probing, attacks, network discovery, and much more. One can also use Scapy to build a Man-in-the-Middle tool that will allow eavesdropping and injection into conversations. (The Defalt, 2015) Even the most 'evil' tools designed purely for breaching security are very useful for benign purposes, such as penetration testing.

Although the act of breaching security measures is 'offensive' in terms of aggression towards the system regardless of the motivation behind it, we need to distinguish the use of such labels in technological areas and in international diplomacy. Although some cyber capabilities can be used for malign purposes, describing them as 'offensive' in strategic documents mirrors a malign intent behind their use.

The misperception of cyber capabilities resulting from incorrect terminology might be one of the reasons behind the tense and secretive environment that surrounds their development, and the unwillingness to discuss their use during operations. NATO and individual allies should therefore abstain from using the harmful label. Just as with the development of new military tools in physical domains, allies should begin an open conversation about cyber tools and dismiss any concerns by political assurance about their exclusive use within NATO's defensive mandate, such as is being done with the development of new physical military arsenals. The resultant transparency amongst allies and their populations shall lead towards

lessening the stigma around cyber capabilities, diminishing secrecy and its overall negative impact, as well as facilitating better understanding of the cyber domain as a whole.

Describing cyber capabilities as "cyber weapons" adds to a similar effect. Cyber capabilities do not necessarily need to be used in such manner, therefore we shall refrain from labelling the development of a certain piece of code as 'weapon development', as its use in an offensive manner solely depends on an intent to do so.

Another hindering approach towards cyber capabilities is the above discussed parallel that links them with nuclear weapons. Such claims are supported by the example of Stuxnet, which made the world aware of the potential ability of cyber capabilities to destroy physical facilities and therefore cause extensive damage. At the same time certain cyber capabilities might, in theory, be able to affect systems controlling the release of nuclear weapons.

This argument also leads us back to the intent of use that determines the cyber capability's scale of effect. Unlike chemical or nuclear weapons, which can only be used in one way, a certain cyber capability can be applied to various targets with precision and cause various outcomes, accordingly to its use. Without targeting a nuclear facility or nuclear weapons themselves, a cyber capability can never cause a physical impact on a nuclear scale.

Of course, certain capabilities combined with malign intent might theoretically result in nuclear catastrophe. However, this borderline scenario is not sufficient to design an approach to the whole concept of cyber capabilities. Physical capabilities are not classified by their most malicious use possible – for example, ballistic missiles might be used to target a nuclear facility, yet they are not generally approached as dirty bombs. Putting the whole concept of cyber capabilities onto the 'nuclear level' therefore protracts the incomprehension of cyberspace.

In order to lead open conversation about cyber capabilities, it would be necessary to acknowledge the existence of tools with such powerful abilities and operations with intent to cause such significant consequences. However, in order not to suffocate the entire debate about cyber capabilities with such extreme cases, it would be important to introduce a classification of the concept. This classification should reflect not only the potential strength of the capability, but also its application and intent. Although it might come over as a little vague, it still should be able to separate the most severe cases of use of cyber capabilities from the lower-scale cyber operations that will soon dominate the battlefield.

There is an example of such categorisation hidden in the de-classified US Presidential Policy Directive 20, which deals with the subject of US cyber operations policy. The Directive distinguishes a category of operations that are reasonably likely to result in 'significant consequences'; this term meaning: 'loss of life, significant responsive actions against the United States, significant damage to property, serious adverse US foreign policy consequences, or serious economic impact on the United States'. The launch of operations likely to result in such consequences needs to be approved by the President of the United States, while in other cyber operations the Directive does not 'intend to alter existing procedures, guidelines, or authorities for cyber collection'.

Although this paragraph deals mainly with cyber espionage operations, the underlying message can be transferred to other types of operations as well. If NATO introduces a

differentiated concept of cyber capabilities, it might liberate the inter-ally debate about their development. Although there will probably still be a blanket of secrecy overlaying certain vulnerabilities and powerful advance persistent threats (APTs) designed for their exploitation, the stigma might be taken away from cyber capabilities as a general concept, thus partially freeing a discussion about the topic. It will enable allies to effectively address the development and use of cyber elements in warfare.

There is one more argument being made behind the asserted parallel between nuclear and cyber capabilities: the element of uncertainty when it comes to the impact of cyber capabilities in cyberspace as an interconnected realm, which might result in unforeseen consequences. Such uncertainty is sometimes said to ascribe potentially significant consequences to all cyber capabilities. As Markus Kont from CCD COE puts it, modern IT systems are highly complex, can be interconnected to an unforeseeable degree, and are built on long chains of dependencies. Thus, breaking one component can indeed have unforeseeable consequences. However, cyber operations on a state or international level incorporate vast assurance processes before the use of cyber capabilities is even considered – a process called 'cyber damage assessment' that is able to predict the operation outcomes to a high degree (Denning, 2015). It is, of course, not possible to assure the outcome of a cyber operation with absolute certainty; but 'absolute certainty' is not present when it comes to the use of any coercive measures, regardless of their physical, cyber, political or economic nature.

Before any cyber operation is conducted, states determine its effect and the level of force that it will represent. They are also responsible for predicting whether or not those effects will rise to the level of force in traditional military domains; the *Tallinn Manual 2.0* provides guidance for such assessment (Denning, 2015; Schmitt, 2015). If it was truly impossible for states to assess the effects of a cyber attack to a sufficient degree, we could not have sought to conduct such assessment, or even have banned certain targets of cyber capabilities (as the *Tallinn Manual 2.0* does); we would have ban all the cyber capabilities at once.

Viewing the concept of cyber capabilities through an absolute and somewhat fatalist optics of nuclear weapons is incorrect on many levels, and distorts comprehension of the concept. This results in multiple threats to NATO. First, combining incomprehension of the nature of cyber capabilities with negative connotations of the 'nuclear' area might generate further unwillingness to debate their use, and unwillingness to opt for cyber solutions during operations, although they might be more efficient. Second, the unwillingness to deploy cyber capabilities will subsequently translate into lowered deterrence potential in cyberspace, if there is any at the moment.

# 6. Conclusion and recommendations

## 6.1. Conclusion

This paper presents an analysis of cyberspace as a domain of operations through the framework of a SWOT analysis. In this section, I will summarise the arguments stemming from the respective parts, which all combine to address the possible future impact on NATO of recognising cyberspace as a domain of operations.

The paper has identified three strengths stemming from cyberspace's position as a domain of operations: strengthened cooperation in cyberspace and its deeper embodiment into military ethos; newfound emphasis on the importance of cyberspace as a realm of warfare together with discourse of mutual help in development; and a possible increase of the Alliance's overall deterrence and a strong message to adversaries that NATO is prepared for the warfare of the future.

Second, the paper presented the current weaknesses of the new domain. These are: the current lack of trust and unity within the Alliance; unresponsiveness to cyber attacks; the attribution problem; the capability gap between NATO members; and relative incomprehension of cyberspace and its concepts from a non-technological point of view.

Making cyberspace a domain of operations has also resulted in multitude of opportunities. With its new-found focus on cyberspace, NATO has a chance to accelerate development in the area and expand its range of capabilities needed for mission assurance. Through increased pressure to do so, NATO can further motivate less cyber-capable states into strengthening their cyber defence and building their cyber capacities. In turn, the Alliance might strengthen as a whole, and its deterrent potential might increase. It is also possible that narrowing the capability gap might contribute to reducing the secrecy amongst allies that has resulted from a recent inability of certain states to handle sensitive information. Establishing cyberspace as a domain might represent an incentive for a non-technological debate on cyberspace and its concepts.

However, the future development in the new domain might not necessarily be positive. NATO is facing four major threats in cyberspace. First is a possible slow decay of the Alliance due to increase in mutual mistrust amongst NATO members. Such a development could be triggered by inability or unwillingness to respond to cyber-attacks, and further protracted by the overall atmosphere of secrecy regarding development of cyber capabilities. These substantial problems subsequently translate into lack of unity in NATO and thus threaten to make it significantly weaker. The second threat represents the problematic attribution of cyber attacks and allies' unwillingness to respond to them, which potentially makes cyberspace a domain of choice for attackers. Third, future weakening of the Alliance might be caused by further widening of the capability gap, if NATO fails to ensure its closure. Having numerous 'weak-link' states in the Alliance will pose a significant security threat to NATO due to its interconnectedness, and might also halt future operations. The fourth threat stems from a possibly unforeseen problem: incomprehension of certain concepts from the non-technological perspective on cyberspace. As shown in theory and practical examples, mishandling important concepts results in strategic inaccuracy and confusion which, if translated into strategic documents, might subsequently cause NATO not to fulfil its defensive potential in cyberspace.

### 6.2. Recommendations

To fully take advantage of the opportunities and avoid the threats, the paper presents several recommendations.

NATO should embrace the strengths of elevating cyberspace onto the level of a domain of operations. It should use the now enlarged space for cooperation to enhance development in cyberspace. This development should be directed primarily towards the states which

possess lesser cyber abilities; to help them with development in cyberspace, NATO might consider developing a framework of procedures on how to develop a viable cyber defence. Outlining the process step by step will make it easier for states to secure their (and the Alliance's) cyberspace. Accelerating cyber development in the less capable states will be a direct contribution to strengthening NATO's cyberspace as a whole.

However, if member states themselves are not willing to allocate resources to cyberspace, development in the area will stall. NATO should therefore consider a further political push on cyberspace development by establishing a minimum spending on cyber within the 2% GDP military spending threshold. Although the spending requirements are not mandatory and thus are not an absolute guarantee of finance allocation to cyber, such a threshold might at least facilitate political debate over spending on cyber at governmental level within the member states.

NATO should also continue the political pressure for cyber development through the power of political discourse. It is essential for the Alliance to continuously increase its level of preparedness in cyberspace, thus it is vital to continue reminding national decision-makers of the necessity of doing so.

These three recommendations – introducing a development framework, establishing a cyber spending target, and continuing political pressure for development – might help to achieve the reduction of the cyber capability gap and thus strengthen the Alliance as a whole. The paper also presumes that, through creating a more equal cyber security environment within the Alliance, allies themselves will be less prone to secrecy due to reduced potential for mishandling the information. A further push from scholars on lessening the secrecy would be also vital for this cause. The resulting openness and subsequent enhanced cooperation would also contribute to diminishing the threat to the Alliance's unity and mutual trust.

NATO should also use the cyber domain's momentum to take the opportunity to overcome the lack of theory and concepts within non-technological knowledge about the field. It is necessary for NATO researchers to address this weakness and approach cyberspace with both a fresh and a critical eye. It is essential to consider all the specifics of the new domain. Hopefully, we will witness an entirely new wave of non-technological academic debate on cyberspace, resulting in an enhanced non-technological comprehension of cyberspace that will subsequently allow decision-makers and the political sphere in general to grasp the concepts much better and hence make more informed decisions.

Profound understanding of the cyber domain should also facilitate an open discussion about cyberspace, its capabilities and their development; a target that NATO should also strive to reach. Reduction of secrecy will enable allies to build their defence collectively and thus strengthen the entire Alliance. As outlined in the paper, some of the reasons behind the secrecy result from an incorrect grasp of the concepts; therefore, they can be dealt with by further research and debate.

Lifting the stigma from cyber capabilities, combined with a greater understanding of the entire concept, will also result in higher likelihood of their use during operations. NATO should follow this trend, as cyber capabilities promise to be a less destructive and less costly alternative to physical military means. Exploring the full potential of their use during operations should be a high priority for NATO. However, such a process can only work if the

Alliance – and individual allies –give up their obstructive, overly-secretive approach towards the domain.

If NATO is to be able to embrace cooperation and development in cyberspace, clear the conceptual confusions, and start an open discussion about cyberspace and the use of its elements during operations, it might be able to reduce what can be perceived as the ultimate threat to the Alliance – loss of its unity. There are some inherent problems to cyberspace that will continue to hinder mutual trust among the allies, such as the attribution problem or inability to define the red line that evocates collective response. However, by dealing with all the other threats and weaknesses, and by taking up the opportunities, NATO can minimise the negative effects of those inherent problems.

Cyberspace is a unique domain. Its development is dizzyingly fast-paced, it empowers non-state actors, it blurs the boundaries between tension and conflict, and most importantly it underlies every physical domain. Being able to defend itself in cyberspace is increasingly becoming a vital need for the Alliance. At the same time, cyberspace offers many opportunities to make the warfare more ethical, more precise and less expensive (from both financial and political perspectives), and to make NATO stronger as a whole. NATO should therefore fully embrace development and cooperation in cyberspace, and it should do so with openness, clarity and emphasis on mutual help. During the process, however, NATO should not forget about the importance of the comprehension of cyberspace from the non-technological perspective, as the crucial decisions – both on transnational and national levels – will ultimately be political.

## Sources


ACKERMAN, Spencer. (2016). Pentagon admits it is 'looking to accelerate' cyber-attacks against Isis. *The Guardian.* February 29, 2016. Available at: https://www.theguardian.com/world/2016/feb/29/pentagon-admits-cyber-attacks-against-isis

BUZAN, Barry and Ole Weaver, Jaap de Wilde (1998). Security: A New Framework for Analysis. *Lynne Reinner Publishers,* 1998, pp. 239. ISBN: 978-1555877842.

DAVIS, Julie H. (2015). Hacking of Government Computers Exposed 21.5 Million People. *New York Times,* July 9, 2015. Available at: https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

DEFENCE NEWS. (2017). NATO might trigger Article 5 for certain cyber attacks. *Defence News,* May 31, 2017. Available at: https://www.defensenews.com/2017/05/31/nato-might-trigger-article-5-for-certain-cyber attacks/

DENNING, Dorothy E. (2015). Assessing Cyber War. In Blanken, Leo and Hy Rothstein, Jason Lepore, *Assessing War,* Georgetown University Press, 2015, pp. 266-284. Available at http://faculty.nps.edu/dedennin/publications/Assessing%20Cyber%20War.pdf

DENNING, Dorothy E. (2015). Rethinking the Cyber Domain and Deterrence. *Joint Forces 77,* 2nd Quarter, April 2015, pp. 8-15. Available at: http://faculty.nps.edu/dedennin/publications/Rethinking%20the%20Cyber%20Domain%20and%20Deterrence%20-%20jfq-77_8-15.pdf

DOMBROWSKI, Peter and Chris C. Demchak (2014). Cyber War, Cybered Conflict, and the Maritime Domain. *Naval War College Review,* Vol. 67, Is. 2, pp. 71-96, 2014. Available at: https://www.usnwc.edu/getattachment/762be9d8-8bd1-4aaf-8e2f-c0d9574afec8/Cyber-War,-Cybered-Conflict,-and-the-Maritime-Doma.aspx

FARRELL, Henry (2014). The political science of cybersecurity III – How international relations theory shapes U.S. cybersecurity doctrine. *The Washington Post,* February 20, 2014. Available at: https://www.washingtonpost.com/news/monkey-cage/wp/2014/02/20/the-political-science-of-cybersecurity-iii-how-international-relations-theory-shapes-u-s-cybersecurity-doctrine/?utm_term=.1818dece4a47

FREEDMAN, Lawrence (2004). Deterrence. *Cambridge,* MA: Polity Press, 2004. 145 pp. ISBN: 0-7456-3112-6

KNAKE, Robert K. (2015). Data Breach at the Office of Personnel Management: China, Again… Really? *Council on Foreign Relations.* June 05, 2015. Available at: https://www.cfr.org/blog/data-breach-office-personnel-management-china-again-really

KRAMER, Franklin D. and Robert J. BUTLER, Catherine LOTRIONTE. (2016). Cyber, Extended Deterrence, and NATO. *Atlantic Council,* Brent Scowcroft Center on International Security, May 26, 2016. Available at: http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf

LEWIS, James A. (2015). The Role of Offensive Cyber Operations in NATO's Collective Defence. *NATO CCD COE,* The Tallinn Paper No. 8, 2015. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf

LEWIS, James A. (2016). The Rationale for Offensive Cyber Capabilities. *Australian Strategic Policy Institute,* The Strategist, June 2016. Available at: https://www.aspistrategist.org.au/rationale-offensive-cyber-capabilities/

MULLER, Lilly P. and Tim Stevens (2017). Upholding the NATO cyber pledge. *Norweigan Institute of International Affairs,* Policy Brief, May 2017. Available at: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NUPI-Policy_Brief_5_17_LMuller_TStevens.pdf

OCCUPY4ELES. (2016). Use NMAP 7 to Discover Vulnerabilities, Launch DoS Attacks and More. *Null Byte,* Wonder How To. February 02, 2016. Available at: https://null-byte.wonderhowto.com/how-to/use-nmap-7-discover-vulnerabilities-launch-dos-attacks-and-more-0168788/

OLIPHANT, Roland (2017). Ukraine to 'seek Nato membership' as Alliance sends Kiev equipment to fight cyber attacks. *The Telegraph,* July 10, 2017. Available at: http://www.telegraph.co.uk/news/2017/07/10/ukraine-seek-nato-membership-Alliance-sends-kiev-equipment-fight/

PBS (2014). Some experts question evidence North Korea is behind the Sony hack – Part 2. *PBS.* December 23, 2014. Available at: http://www.pbs.org/newshour/bb/debating-north-koreas-involvement-sony-hack/

PERNIK, Piret. 2016. NATO's Cyber Deterrence. *International Centre for Defence and Security,* June 21, 2016. Available at: https://www.icds.ee/fileadmin/media/icds.ee/failid/Piret_Pernik_-_NATO_s_Cyber_Deterrence__June_2016.pdf

SEGAL, Adam (2015). Cyberspace's Other Attribution Problem. *Council on Foreign Relations,* August 5, 2015. Online available at: https://www.cfr.org/blog/cyberspaces-other-attribution-problem

SHACKELFORD, Scott. (2009) From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkley Journal of International Law (BJIL), Vol. 25, No. 3, April 28, 2009. Available at: https://ssrn.com/abstract=1396375

SNYDER, Glenn H. (1961). Deterrence and Defense. *Priceton University Press,* 1961. ISBN: 978-1-4008-7716-4. Available at: http://www.jstor.org/stable/j.ctt183pj49

TAKALA, Rudy (2015). Former spy chief complains about 'hideous over-classification'. *Washington Examiner,* October 28, 2015. Available at: http://www.washingtonexaminer.com/former-spy-chief-complains-about-hideous-over-classification/article/2575161

THE DEFALT. (2015). Build a Man-in-the-Middle Tool with Scapy and Python. *Null Byte,* Wonder How To. July 30, 2015. Available at: https://null-byte.wonderhowto.com/how-to/build-man-middle-tool-with-scapy-and-python-0163525/

TOR, Uri. (2015). Cumulative Deterrence as a New Paradigm for Cyber Deterrence. *Journal of Strategic Studies,* December 18, 2015, pp. 92-117. Available at: http://www.tandfonline.com/doi/abs/10.1080/01402390.2015.1115975

TURNER, Michael (2013). Is There Such a Thing as a Violent Act in Cyberspace. *University of Cambridge,* International Security and Intelligence Summer School, 2013. Available at: http://www.pem.cam.ac.uk/wp-content/uploads/2013/04/Is-there-such-a-thing-as-violence-in-cyberspace.pdf

VERBONCU, Ion and Andreea CONDURACHE (2016). Diagnostics vs. SWOT Analysis. *Review of International Comparative Management,* Vol. 17, Is. 2, May 2016. Available at: http://www.rmci.ase.ro/no17vol2/03.pdf

US Presidential Policy Directive / PPD-20 https://fas.org/irp/offdocs/ppd/ppd-20.pdf

Warsaw Summit Communiqué (2016). http://www.nato.int/cps/en/natohq/official_texts_133169.htm

Tallin Manual 2. 0. 2017, Rule 24, Article 6

Tallin Manual 2.0, Rules 74, 75

Article 2 of the Cyber Defence Pledge (2016) http://www.nato.int/cps/en/natohq/official_texts_133177.htm

Wales Summit Declaration (2014) Paragraph 72 http://www.nato.int/cps/en/natohq/official_texts_133169.htm